

Quantum Strongly Secure Ramp Secret Sharing

Paul Zhang · Ryutaroh Matsumoto

August 8, 2014

Abstract Quantum secret sharing is a scheme for encoding a quantum state (the secret) into multiple shares and distributing them among several participants. If a sufficient number of shares are put together, then the secret can be fully reconstructed. If an insufficient number of shares are put together however, no information about the secret can be revealed. In quantum ramp secret sharing, partial information about the secret is allowed to leak to a set of participants, called an unqualified set, that cannot fully reconstruct the secret. By allowing this, the size of a share can be drastically reduced. This paper introduces a quantum analog of classical strong security in ramp secret sharing schemes. While the ramp secret sharing scheme still leaks partial information about the secret to unqualified sets of participants, the strong security condition ensures that qudits with critical information can no longer be leaked.

Keywords quantum secret sharing · non-perfect secret sharing · ramp secret sharing · strong security

PACS 03.67.Dd

Mathematics Subject Classification (2010) 81P94 · 94A62

1 Introduction

Secret sharing (SS) [11] is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that only *qualified sets* of participants can

Paul Zhang
California Institute of Technology, USA
ORCID: 0000-0003-4136-1315
E-mail: pzpzp1@gmail.com

Ryutaroh Matsumoto
Department of Communications and Computer Engineering
Tokyo Institute of Technology, Japan
ORCID: 0000-0002-5085-8879
E-mail: ryutaroh@it.ce.titech.ac.jp

reconstruct the original secret from their shares. Traditionally both secret and shares were classical information (bits). Several authors [4, 5, 12] extended the traditional SS to a quantum one so that a quantum secret is encoded to quantum shares.

SS can be classified into two categories. One is perfect SS and the other is non-perfect or ramp SS [9], [13, Chapter 13]. In perfect SS, we require every unqualified set of participants to have zero information of the secret, while in non-perfect SS we do not require such a property. A major disadvantage of perfect SS is that the size of each share must be larger than or equal to that of secret, in both classical case [3] and quantum case [4, 5, 12]. By tolerating partial information leakage to unqualified sets, the size of shares can be much smaller than that of secret. Such an SS is called a ramp SS or a non-perfect SS [2, 6, 9, 14]. The quantum ramp SS was proposed by Ogawa et al. [10]. In both Ogawa et al.'s scheme and our proposal, the size of shares is L times smaller than that of the secret, where L is the number of qudits in a secret. This paper focuses only on the quantum ramp SS.

For a general ramp SS, an unqualified set of participants is allowed to have partial information of the secret. This can be undesirable in some cases. For example, consider a classical secret representing “*username : password*”. When an unqualified set has 8-symbol partial information of the secret, it could know all of “*password*”, which is critical confidential information. The existence of such a case is demonstrated in an explicit example by Iwamoto and Yamamoto [6]. The first purpose of this paper is to demonstrate a similar danger in the quantum ramp SS [10] by providing an explicit example.

In order to prevent such cases, Yamamoto [6, 14] defined the strong security of classical ramp SS as follows: A (k, L, n) strongly secure classical ramp SS distributes L symbols of a classical secret s to n symbols such that any k or more participants can determine s while any i symbols of s is kept completely secret to any $(k - i)$ or less participants, where each participant has one symbol. Thus a strongly secure ramp SS excludes the danger explained in the last paragraph.

The second purpose of this paper is to adapt the strong security criterion in the classical case to the quantum case. We define a quantum (k, L, n) strongly secure ramp SS as a quantum ramp SS that distributes L qudits of a quantum secret σ to n qudits ρ such that any k or more participants can determine σ while any i qudits of σ is kept completely secret from any $k - i$ or less participants, where each participant has one qudit.

The third purpose of this paper is to provide an explicit construction of quantum ramp SS realizing the strong security with the same efficiency as the conventional quantum ramp SS in [10]. The difference of constructions between [10] and ours is as follows: While Ogawa et al. [10] encode a secret to coefficients of a polynomial, we encode it to the function values of a polynomial as done in [7, 8] for the construction of classical strongly secure SS.

We stress that this paper studies ramp (non-perfect) SS while [4, 5, 12] studied perfect SS, and that none of the results in this paper are contained in [4, 5, 12].

This paper is organized as follows: Section 2 demonstrates how Ogawa et al.'s encoding fails to satisfy an intuitive quantum version of Yamamoto's classical strong security. Section 3 formalizes the strong security criterion for quantum ramp SS. Section 4 proposes the encoding of secrets. Section 5 proposes the decoding of secrets.

Section 6 proves the strong security of the proposed scheme. Section 7 gives concluding remarks.

2 Motivation for Quantum Strong Security

We will show here how Ogawa et al.'s secret sharing scheme fails to satisfy the strong security condition. Let \mathcal{G}_i and \mathcal{H}_j be q -dimensional complex linear spaces. We refer to quantum systems represented by \mathcal{G}_i and \mathcal{H}_j as *qudits*. We assume q to be a prime power, and denote by \mathbf{F}_q the finite field with q elements. We also assume that orthonormal bases of \mathcal{G}_i and \mathcal{H}_j are indexed by \mathbf{F}_q as $\{|s\rangle\}_{s \in \mathbf{F}_q}$.

In Ogawa et al.'s (k, L, n) ramp secret sharing scheme, the encoding of a quantum secret is defined by unique public values $(x_1, \dots, x_n) \in \mathbf{F}_q^n$ and the transformation of an L -qudit secret $|s_1, \dots, s_L\rangle$, to

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{\mathbf{c} \in D(s^L)} |p_{\mathbf{c}}(x_1), \dots, p_{\mathbf{c}}(x_n)\rangle,$$

where $D(s^L) = \{(c_1, \dots, c_k) \in \mathbf{F}_q^k \mid \forall i \in \{1, \dots, L\} \ c_i = s_i\}$, and $p_{\mathbf{c}}(x) = c_1 + c_2x + \dots + c_{k-L+1}x^{k-L+1}$ the polynomial whose coefficients are specified by $\mathbf{c} = (c_1, \dots, c_k)$. We now provide a specific example in which an unqualified set is able to reconstruct one qudit of the secret.

Example 1 We consider this scheme where the number of qudits in the secret $L = 2$, the minimal number of participants needed to decode the secret $k = 3$, the number of shares $n = 4$, and the size of the field $q = 7$. Public values $\mathbf{x} = (2, 3, 1, 6) \in \mathbf{F}_7^4$. The quantum secret has $q^L = 49$ dimensions. Its orthonormal basis is the set $\{|s_1 s_2\rangle \mid s_1, s_2 \in \mathbf{F}_7\}$.

We choose a particular basis state $|s_1 s_2\rangle$ to be the secret and consider the shares encoded from $|s_1 s_2\rangle$. The set $D(s_1, s_2)$ consists of coefficients $\mathbf{c}_i = (s_1, s_2, r_i)$ where $i \in \{1, \dots, 7\}$ and $r_i = i - 1 \in \mathbf{F}_7$. These coefficients specify polynomials to be in the form:

$$p(x)_i = s_1 + s_2 x + r_i x^2.$$

The four shares, corresponding to $\mathbf{c}_i = (s_1, s_2, r_i)$, are therefore given by

$$\begin{aligned} p_{\mathbf{c}_1}(2) &= s_1 + 2s_2 + 4r_1, \\ p_{\mathbf{c}_1}(3) &= s_1 + 3s_2 + 2r_1, \\ p_{\mathbf{c}_1}(1) &= s_1 + s_2 + r_1, \\ p_{\mathbf{c}_1}(6) &= s_1 + 6s_2 + r_1. \end{aligned}$$

The encoded state of four shares is

$$\begin{aligned} &\frac{1}{\sqrt{7}}(|p_{\mathbf{c}_1}(2), p_{\mathbf{c}_1}(3), p_{\mathbf{c}_1}(1), p_{\mathbf{c}_1}(6)\rangle + |p_{\mathbf{c}_2}(2), p_{\mathbf{c}_2}(3), p_{\mathbf{c}_2}(1), p_{\mathbf{c}_2}(6)\rangle + \\ &\quad |p_{\mathbf{c}_3}(2), p_{\mathbf{c}_3}(3), p_{\mathbf{c}_3}(1), p_{\mathbf{c}_3}(6)\rangle + |p_{\mathbf{c}_4}(2), p_{\mathbf{c}_4}(3), p_{\mathbf{c}_4}(1), p_{\mathbf{c}_4}(6)\rangle + \\ &\quad |p_{\mathbf{c}_5}(2), p_{\mathbf{c}_5}(3), p_{\mathbf{c}_5}(1), p_{\mathbf{c}_5}(6)\rangle + |p_{\mathbf{c}_6}(2), p_{\mathbf{c}_6}(3), p_{\mathbf{c}_6}(1), p_{\mathbf{c}_6}(6)\rangle + \\ &\quad |p_{\mathbf{c}_7}(2), p_{\mathbf{c}_7}(3), p_{\mathbf{c}_7}(1), p_{\mathbf{c}_7}(6)\rangle). \end{aligned}$$

Since $1^2 = (-1)^2 = 6^2 = 1 \in \mathbb{F}_7$, the coefficients of r_i in the 3rd and the 4th shares are both 1, which provides us with the classical equation

$$s_2 = 4p(1)_i - 4p(6)_i. \quad (1)$$

This shows that the value s_2 can be retrieved using information from the 3rd and 4th participants. In the quantum setting, the 3rd and the 4th participants can collectively apply a unitary matrix \mathcal{U} based on (1) to produce $|s_2\rangle$ (entangled with the rest of the shares).

A full rank matrix that performs our desired classical transformation is

$$M = \begin{pmatrix} 4 & 4 \\ -4 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 4 \\ 3 & 4 \end{pmatrix}.$$

This classical transformation performs a change of basis indices for our quantum state. The unitary quantum transformation \mathcal{U} , corresponding to M , sends $|p_{\mathbf{c}}(1), p_{\mathbf{c}}(6)\rangle$ of the 3rd and 4th participants to

$$|(p_{\mathbf{c}}(1), p_{\mathbf{c}}(6)) \cdot M\rangle = |s_2, s_1 + r_i\rangle.$$

\mathcal{U} is unitary because it just permutes basis vectors.

After applying such a transformation on the 3rd and 4th shares, a measurement in the basis $\{|0\rangle, \dots, |6\rangle\}$ can read off the index s_2 . If the s_2 -component of the quantum secret happens to be classical information, then it can be completely read off by the 3rd and the 4th participants. Therefore two shares (an unqualified set) are capable of obtaining partial information of the secret. The strong security condition exists to make sure that no qudits of critical information can be revealed to an unqualified set of participants. Therefore, Ogawa et al.'s encoding is not a strongly secure ramp secret sharing scheme.

Also observe that the 3rd and the 4th participants can figure out s_2 even when the first qudit $|s_1\rangle\langle s_1|$ is the fully mixed state $I_{7 \times 7}/7$ as in Definition 1.

3 Definition of the Strong Security

To formally define quantum strong security, we use the same \mathcal{G}_i and \mathcal{H}_j as earlier.

Definition 1 For integers $0 < L < k < n$, we define a quantum (k, L, n) -threshold strongly secure ramp secret sharing scheme as a completely positive trace-preserving map [1, Chapter 8] W of σ on the state space $\mathcal{S}(\bigotimes_{i=1}^L \mathcal{G}_i)$ into $\mathcal{S}(\bigotimes_{j=1}^n \mathcal{H}_j)$ with the following conditions.

1. σ can be reconstructed from any k or more qudits of \mathcal{H}_j .
2. Let $\mathcal{I} \subseteq \{1, \dots, L\}$, $\overline{\mathcal{I}} = \{1, \dots, L\} \setminus \mathcal{I}$, $\sigma_1 \in \mathcal{S}(\bigotimes_{i \in \mathcal{I}} \mathcal{G}_i)$, $\rho_{\text{mix}, \overline{\mathcal{I}}}$ the fully mixed state in $\mathcal{S}(\bigotimes_{i \in \overline{\mathcal{I}}} \mathcal{G}_i)$, $\mathcal{J} \subset \{1, \dots, n\}$, and $\overline{\mathcal{J}} = \{1, \dots, n\} \setminus \mathcal{J}$. If $|\mathcal{J}| \leq k - |\mathcal{I}|$, then $\text{Tr}_{\bigotimes_{j \in \overline{\mathcal{J}}} \mathcal{H}_j} W(\sigma_1 \otimes \rho_{\text{mix}, \overline{\mathcal{I}}})$ is independent of σ_1 . In other words, no quantum information of σ_1 is leaked to shares whose indices belong to \mathcal{J} .

Observe that σ represents a quantum secret and n qudits in $\mathcal{S}(\bigotimes_{j=1}^n \mathcal{H}_j)$ represent n shares distributed to n participants. Note, Condition 2 with $I = \{1, \dots, L\}$ is equivalent to the conventional security definition [10, Definition 1]. In Condition 2, we assume that the unqualified set of participants represented by \mathcal{J} has no prior knowledge on the quantum state on \bar{I} . This lack of prior knowledge is expressed as the fully mixed state $\rho_{\text{mix}, \bar{I}}$ in $\mathcal{S}(\bigotimes_{i \in \bar{I}} \mathcal{G}_i)$.

When the quantum secret is an output of a nearly optimal quantum data compression [1, Section 12.2.2], then the output is close to the fully mixed state, otherwise it allows further compression. The fully mixed state in Condition 2 is also justified in such a case.

4 Encoding Secrets

We will propose an explicit construction satisfying the conditions of the last section. Our proposal is a quantum version of classical strongly secure secret sharing [7, 8]. As in [10] we set $n = 2k - L$ indicating a pure state quantum secret sharing scheme.

Let \mathbf{F}_q be as it was previously. Let $x_1, \dots, x_L, y_1, \dots, y_n$ denote publicly known pairwise distinct elements in \mathbf{F}_q . Let D_k be equivalent to \mathbf{F}_q^k with an interpretation as the set of coefficients of univariate polynomials over \mathbf{F}_q with degree less than k . For $\mathbf{u} = (u_1, \dots, u_\ell) \in \mathbf{F}_q^\ell$ with pairwise distinct u_1, \dots, u_ℓ and $\mathbf{c} \in D_k$, define $P_{\mathbf{c}}(\mathbf{u}) = (p_{\mathbf{c}}(u_1), \dots, p_{\mathbf{c}}(u_\ell)) \in \mathbf{F}_q^\ell$ to be the evaluation of a polynomial specified by \mathbf{c} , at points u_1, \dots, u_ℓ .

Ogawa et al. [10, Lemma 3] proved the following lemma:

Lemma 1 *Given a vector $\mathbf{A} \in \mathbf{F}_q^m$ whose elements are pairwise unique, the map $\mathbf{c} \in D_k \mapsto P_{\mathbf{c}}(\mathbf{A}) \in \mathbf{F}_q^m$ is injective if $m \geq k$, and it is bijective if $m = k$.*

Denote (x_1, \dots, x_L) by \mathbf{x} and (y_1, \dots, y_n) by \mathbf{y} , and let $D_k(\mathbf{s}) = \{\mathbf{c} \in D_k \mid P_{\mathbf{c}}(\mathbf{x}) = \mathbf{s}\}$ for $\mathbf{s} \in \mathbf{F}_q^L$. By Lemma 1 we see $|D_k(\mathbf{s})| = q^{k-L}$. Consider the encoding map W sending $|s_1, s_2, \dots, s_L\rangle \in \bigotimes_{i=1}^L \mathcal{G}_i$ to

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{\mathbf{c} \in D_k(s_1, \dots, s_L)} |P_{\mathbf{c}}(\mathbf{y})\rangle \in \bigotimes_{j=1}^n \mathcal{H}_j, \quad (2)$$

where $s_i \in \mathbf{F}_q$. This map embeds an orthonormal basis of $\bigotimes_{i=1}^L \mathcal{G}_i$ into that of $\bigotimes_{j=1}^n \mathcal{H}_j$. So this map can be uniquely extended to a complex linear isometric embedding from $\bigotimes_{i=1}^L \mathcal{G}_i$ into $\bigotimes_{j=1}^n \mathcal{H}_j$.

Observe that the sizes of a secret and shares are the same as those of the conventional quantum ramp secret sharing scheme by Ogawa et al. [10], which means the coding rate of our proposal is also optimal in the sense of [10, Corollary 2].

Example 2 As a concrete case, we use the following ($k = 3, L = 2, n = 4$) quantum ramp secret sharing scheme to encode a secret. Let $|\mathbf{s}\rangle = |1, 5\rangle$ be the secret that

we wish to encode. We set the publicly known values \mathbf{x} and \mathbf{y} to be $\mathbf{x} = (1, 3)$, and $\mathbf{y} = (6, 2, 4, 5)$. The set $D_3(1, 5)$ can now be calculated explicitly as

$$D_3(1, 5) = \left\{ \begin{matrix} (6, 2, 0), (2, 5, 1), (5, 1, 2), \\ (1, 4, 3), (4, 0, 4), (0, 3, 5), (3, 6, 6) \end{matrix} \right\}. \quad (3)$$

One can verify that each element \mathbf{c} of $D_3(1, 5)$ has the property that $s_i = c_1 + c_2 x_i + c_3 x_i^2$, as well as the fact that no other polynomials have the same property.

The encoded secret is the superposition of states indexed by evaluations of polynomials specified by \mathbf{c} , on \mathbf{y} . We show explicitly that the state corresponding to $\mathbf{c} = (2, 5, 1)$, is $|5, 2, 3, 3\rangle$ by the following calculation.

$$\begin{aligned} 2 + 5y_1 + y_1^2 &= 2 + 5 * 6 + 6^2 = 2 - 5 + 1 &= 5 \\ 2 + 5y_2 + y_2^2 &= 2 + 5 * 2 + 2^2 = 16 &= 2 \\ 2 + 5y_3 + y_3^2 &= 2 + 5 * 4 + 4^2 = 2 + 20 + 16 = 38 &= 3 \\ 2 + 5y_4 + y_4^2 &= 2 + 5 * 5 + 5^2 = 2 + 25 + 25 &= 3 \end{aligned}$$

One can verify that the states, corresponding to all $\mathbf{c} \in D_k(1, 5)$, in the same order as presented in (3), are

$$\begin{aligned} &|4, 3, 0, 2\rangle, |5, 2, 3, 3\rangle, |6, 1, 6, 4\rangle, \\ &|0, 0, 2, 5\rangle, |1, 6, 5, 6\rangle, |2, 5, 1, 0\rangle, |3, 4, 4, 1\rangle. \end{aligned}$$

The final encoded state is therefore given by

$$\begin{aligned} |\psi_{ex}\rangle &= \frac{1}{\sqrt{7}}(|4, 3, 0, 2\rangle + |5, 2, 3, 3\rangle + |6, 1, 6, 4\rangle + \\ &|0, 0, 2, 5\rangle + |1, 6, 5, 6\rangle + |2, 5, 1, 0\rangle + |3, 4, 4, 1\rangle). \end{aligned} \quad (4)$$

Note that if we looked at the subsystem on the last qudit, we have only a fully mixed state. In general, if we looked at any $n - k$ qudit subsystem of the encoded state, we would only find a fully mixed state. We will prove this important fact as (11) in Section 5.

5 Decoding Secrets

In this section we will show that by performing the unitary transformations in [10, Section VII] with suitable modifications, k or more participants can decode the quantum secret $|\mathbf{s} = (s_1, \dots, s_L)\rangle$. As [10, Section VII], we assume that the number of participants is exactly k .

Let the notation A_B , where $A \in \mathbb{F}_q^m$ is a vector and $B \subseteq \{1, \dots, m\}$ is an ordered ascending set, be $(a_{b_1}, a_{b_2}, \dots, a_{b_{|B|}})$ the vector A indexed by B . Let $\mathcal{J} \subset \{1, \dots, n\}$, where $|\mathcal{J}| = k$, be the set indexing the shares available to the k participants, and $\overline{\mathcal{J}} = \{1, \dots, n\} \setminus \mathcal{J}$. Now we introduce slightly modified notation from [10]:

$$M_d^c(A_B) = \begin{pmatrix} a_{b_1}^c & \dots & a_{b_{|B|}}^c \\ a_{b_1}^{c+1} & \dots & a_{b_{|B|}}^{c+1} \\ \vdots & & \vdots \\ a_{b_1}^d & \dots & a_{b_{|B|}}^d \end{pmatrix} \quad (c < d).$$

This is generally a submatrix of a Vandermonde matrix. Note that $M_{k-1}^0(A_B)$ acts as the linear transformation between the coefficients \mathbf{c} of a polynomial of degree $k-1$ to its evaluations on the set A_B , that is,

$$\begin{aligned} \mathbf{c} \cdot M_{k-1}^0(A_B) &= \mathbf{c} \begin{pmatrix} a_{b_1}^0 & \dots & a_{b_{|B|}}^0 \\ a_{b_1}^1 & \dots & a_{b_{|B|}}^1 \\ \vdots & & \vdots \\ a_{b_1}^{k-1} & \dots & a_{b_{|B|}}^{k-1} \end{pmatrix} \\ &= \begin{pmatrix} c_0 a_{b_1}^0 & \dots & c_0 a_{b_{|B|}}^0 \\ + & & + \\ c_1 a_{b_1}^1 & \dots & c_1 a_{b_{|B|}}^1 \\ + & & + \\ \vdots & & \vdots \\ + & & + \\ c_{k-1} a_{b_1}^{k-1} & \dots & c_{k-1} a_{b_{|B|}}^{k-1} \end{pmatrix} \\ &= (p_{\mathbf{c}}(a_{b_1}), \dots, p_{\mathbf{c}}(a_{b_{|B|}})) \\ &= P_{\mathbf{c}}(A_B). \end{aligned}$$

This also means, by Lemma 1, that, if $|A_B| = k$, the matrix $M_{k-1}^0(A_B)$ can be inverted to retrieve coefficients \mathbf{c} from $P_{\mathbf{c}}(A_B)$.

As [10], without loss of generality, we let $\mathcal{J} = \{1, \dots, k\}$. Starting with the encoded state (2), we apply the unitary corresponding (review Example 1 for the correspondence) to the first decoding matrix

$$M_{k-1}^0(\mathbf{y}_{\mathcal{J}})^{-1} \quad (5)$$

on shares indexed by \mathcal{J} . As explained above, this transformation will retrieve the polynomial coefficients \mathbf{c} from $P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})$. The resulting state is

$$\frac{1}{\sqrt{q^{k-L}}} \sum_{\mathbf{c} \in D_k(\mathbf{s})} |\mathbf{c}, P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle. \quad (6)$$

Next apply the unitary transformation corresponding to the second decoding matrix:

$$\left(M_{k-1}^0(\mathbf{x}) \quad M_{k-1}^0(\mathbf{y}_{\mathcal{J}}) \right). \quad (7)$$

Note that since $n-k = k-L$, the width of (7) is $|\mathbf{x}| + |\mathbf{y}_{\mathcal{J}}| = (L) + (n-k) = L+k-L = k$. This matrix has the effect of taking coefficients \mathbf{c} and evaluating them at \mathbf{x} and $\mathbf{y}_{\mathcal{J}}$. By our definition of $D_k(\mathbf{s})$, the evaluation of the coefficients at \mathbf{x} , is equivalent to the secret. Therefore, the transformation (7) takes the state in (6) to the final state:

$$\frac{1}{\sqrt{q^{k-L}}} |\mathbf{s}\rangle \otimes \sum_{\mathbf{c} \in D_k(\mathbf{s})} |P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}}), P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle. \quad (8)$$

It remains to verify that the $n - L$ shares left over do not in fact rely on the decoded secret at all. This step is necessary because, if there is any dependency between the decoded secret $|\mathbf{s}\rangle$ and the remaining $n - L$ shares, the decoded secret will no longer be unentangled from the remaining shares when the secret is a superposition of two different pure states $|\mathbf{s}_1\rangle$ and $|\mathbf{s}_2\rangle$. For example, if the decoding on the encoded pure state secret $|\mathbf{s}_1\rangle$ produced a dependence by the shares, on the secret, $|\mathbf{s}_1, f(\mathbf{s}_1)\rangle$, then the decoding of shares encoded from $\frac{1}{\sqrt{2}}(|\mathbf{s}_1\rangle + |\mathbf{s}_2\rangle)$ will be

$$\frac{1}{\sqrt{2}}(|\mathbf{s}_1, f(\mathbf{s}_1)\rangle + |\mathbf{s}_2, f(\mathbf{s}_2)\rangle), \quad (9)$$

which has a different density operator from the one we desire. We need the decoded secret to be unentangled with the remaining shares, resulting in a state

$$\frac{1}{2}(|\mathbf{s}_1\rangle + |\mathbf{s}_2\rangle)(\langle\mathbf{s}_1| + \langle\mathbf{s}_2|) \otimes \rho, \quad (10)$$

where ρ is the density operator of the remaining $n - L$ shares. Thus to show our decoder successfully decodes the secret, we will prove that the quantum state of the remaining shares have no dependence on the secret.

First we prove that for a set $X \subseteq \mathbf{F}_q \setminus \{x_1, \dots, x_L\}$ the map $\mathbf{c} \in D_k(\mathbf{s}) \rightarrow P_{\mathbf{c}}(X)$, where $|X| = k - L$, is bijective. This can be seen in the forward direction by the fact that \mathbf{c} uniquely determines the polynomial's evaluations. In the reverse direction, \mathbf{s} provides us with L evaluations of the polynomial that, when coupled with $|X|$ more evaluations at distinct points, provides us with k evaluations of the polynomial. By applying Lemma 1 the k evaluations uniquely determine the coefficients. Therefore the map between $\mathbf{c} \in D_k(\mathbf{s})$ and $P_{\mathbf{c}}(X)$ for a fixed $\mathbf{s} \in \mathbf{F}_q^L$ is bijective.

We now replace the set X with $\mathbf{y}_{\overline{\mathcal{J}}}$. Since $|D_k(\mathbf{s})| = q^{k-L}$, (8) can now be re-written as

$$\frac{1}{\sqrt{q^{k-L}}}|\mathbf{s}\rangle \otimes \sum_{\mathbf{v} \in \mathbf{F}_q^{k-L}} |\mathbf{v}\rangle |\mathbf{v}\rangle. \quad (11)$$

The remaining $n - L$ shares are therefore a purification of the fully mixed state on the $\overline{\mathcal{J}}$ subsystem. Since it is unentangled with the first L shares, we have reconstructed the secret.

Example 3 We will now provide a concrete example of the decoding scheme acting on our previously calculated encoded state $|\psi_{ex}\rangle$ in (4). Recall that the secret we encoded was $|1, 5\rangle$. First we apply the unitary corresponding to $M_{k-1}^0(Y_{\mathcal{J}})^{-1}$. The matrix $M_{k-1}^0(Y_{\mathcal{J}})$ and its inverse are shown below.

$$M_2^0(6, 2, 4) = \begin{pmatrix} 1 & 1 & 1 \\ 6 & 2 & 4 \\ 6^2 & 2^2 & 4^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 6 & 2 & 4 \\ 1 & 4 & 2 \end{pmatrix} \quad (12)$$

$$M_2^0(6, 2, 4)^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 3 & 4 & 1 \\ 4 & 2 & 5 \end{pmatrix} \quad (13)$$

One can verify that the product of (12) and (13) is the identity.

We explicitly show that the result of (13) acting on state $|4, 3, 0, 2\rangle$ results in $|6, 2, 0, 2\rangle$.

$$(4, 3, 0) \begin{pmatrix} 1 & 1 & 1 \\ 3 & 4 & 1 \\ 4 & 2 & 5 \end{pmatrix} = (4 + 9 + 0, 4 + 12 + 0, 4 + 3) = (6, 2, 0)$$

From Example 2, one can see that $(\mathbf{c}, P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})) = (6, 2, 0, 2)$. One can verify (13) acts similarly for the rest of the terms in (4), resulting in the following partially decoded state:

$$|\psi_{pd}\rangle = \frac{1}{\sqrt{7}}(|6, 2, 0, 2\rangle + |2, 5, 1, 3\rangle + |5, 1, 2, 4\rangle + |1, 4, 3, 5\rangle + |4, 0, 4, 6\rangle + |0, 3, 5, 0\rangle + |3, 6, 6, 1\rangle) \quad (14)$$

The second part of the decoding is to apply (7), which is explicitly evaluated to:

$$(M_{k-1}^0(\mathbf{x}) M_{k-1}^0(\mathbf{y}_{\mathcal{J}})) = M_2^0(|1, 3, 6\rangle) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 5 \\ 1 & 3^2 & 5^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 5 \\ 1 & 2 & 4 \end{pmatrix}. \quad (15)$$

We verify that applying (15) to the state $|5, 1, 2, 4\rangle$ results in $|1, 5, 4, 4\rangle$ below.

$$(5, 1, 2) \begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 5 \\ 1 & 2 & 4 \end{pmatrix} = (5 + 1 + 2, 5 + 3 + 4, 5 + 5 + 8) = (1, 5, 4)$$

One can finish verifying that applying (15) to the state $|\psi_{pd}\rangle$ results in:

$$\begin{aligned} |\psi_{pd}\rangle &= \frac{1}{\sqrt{7}}(|1, 5, 2, 2\rangle + |1, 5, 3, 3\rangle + |1, 5, 4, 4\rangle + \\ &\quad |1, 5, 5, 5\rangle + |1, 5, 6, 6\rangle + |1, 5, 0, 0\rangle + |1, 5, 1, 1\rangle) \\ &= \frac{1}{\sqrt{7}}|1, 5\rangle \otimes \sum_{e \in \mathbb{F}_q} |e, e\rangle \end{aligned} \quad (16)$$

The original secret has now been reconstructed in the first 2 qudits, and the rest of the shares form only a purification of a fully mixed state that is independent of and unentangled with the secret. Therefore the decoding is finished.

6 Strong Security of the Encoder

In order to prove that the proposed encoding method satisfies the definition of quantum strong security, we prove Condition 2 of Definition 1 holds for our encoder.

Let $\mathcal{J} \subset \{1, \dots, n\}$ be the indices of the shares available, and $\mathcal{I} \subset \{1, \dots, L\}$ be the indices of qudits of the secret, where $|\mathcal{J}| = k - i$ and $|\mathcal{I}| = i$. Let the secret on \mathcal{I} be a general pure state

$$|\mathbf{s}_{\mathcal{I}}\rangle = \sum_{\mathbf{s} \in \mathbb{F}_q^i} a_{\mathbf{s}} |\mathbf{s}\rangle, \quad (17)$$

where $a_{\mathbf{s}} \in \mathbb{C}$ and $\sum_{\mathbf{s} \in \mathbb{F}_q^L} |a_{\mathbf{s}}|^2 = 1$. The secret to be encoded is $\rho_{\text{mix}, \bar{\mathcal{I}}} \otimes |\mathbf{s}_{\mathcal{I}}\rangle\langle\mathbf{s}_{\mathcal{I}}|$, representing the secret on indices \mathcal{I} and the fully mixed state in $\mathcal{S}(\bigotimes_{i \in \bar{\mathcal{I}}} \mathcal{G}_i)$ on indices $\bar{\mathcal{I}}$. We will show that $\text{Tr}_{\bigotimes_{j \in \mathcal{J}} \mathcal{H}_j} W(\rho_{\text{mix}, \bar{\mathcal{I}}} \otimes |\mathbf{s}_{\mathcal{I}}\rangle\langle\mathbf{s}_{\mathcal{I}}|)$ is the fully mixed state in $\mathcal{S}(\bigotimes_{j \in \mathcal{J}} \mathcal{H}_j)$, and therefore independent of $|\mathbf{s}_{\mathcal{I}}\rangle$.

For ease of exposition, we purify our secret by introducing a reference system of $|\bar{\mathcal{I}}|$ qudits. The purified secret is therefore equal to:

$$|\psi_{\text{sec}}\rangle = \left(\frac{1}{\sqrt{q^{|\bar{\mathcal{I}}|}}} \sum_{\mathbf{d} \in \mathbb{F}_q^{L-i}} |\mathbf{d}\rangle \otimes |\mathbf{d}\rangle \right) \otimes |\mathbf{s}_{\mathcal{I}}\rangle. \quad (18)$$

The reference system will henceforth be indexed by $\bar{\mathcal{I}}_2$. Let \mathcal{R}_i be q -dimensional complex linear spaces, representing qudits on the reference system.

We act on the space $\bigotimes_{i \in \{1, \dots, L\}} \mathcal{G}_i$ with our encoder. The reference system will remain untouched throughout the proof and be traced out at the end. We denote the n qudits that result from applying our encoder, as “encoded shares”. We now define spaces $A = \left(\bigotimes_{i \in \bar{\mathcal{I}}_2} \mathcal{R}_i \right) \otimes \left(\bigotimes_{j \in \mathcal{J}} \mathcal{H}_j \right)$ and $B = \bigotimes_{j \in \mathcal{J}} \mathcal{H}_j$. Together, A and B form the space in which the encoded shares and reference system reside. The entire scheme can be seen in Figure 1.

Since the reference system is untouched, we can re-express the encoded shares indexed by \mathcal{J} as

$$\begin{aligned} & \text{Tr}_{\bigotimes_{j \in \mathcal{J}} \mathcal{H}_j} W(\rho_{\text{mix}, \bar{\mathcal{I}}} \otimes |\mathbf{s}_{\mathcal{I}}\rangle\langle\mathbf{s}_{\mathcal{I}}|) \\ &= \text{Tr}_A W'(|\psi_{\text{sec}}\rangle\langle\psi_{\text{sec}}|), \end{aligned} \quad (19)$$

where $W' = I \otimes W$ is the full encoding.

Applying W' to the purified secret (18) results in the transformation from $|\psi_{\text{sec}}\rangle$ to:

$$\begin{aligned} |\psi_{\text{enc}}\rangle &= \frac{1}{\sqrt{q^{L-i}}} \sum_{\mathbf{s} \in \mathbb{F}_q^i} a_{\mathbf{s}} \left(\sum_{\mathbf{d} \in \mathbb{F}_q^{L-i}} |\mathbf{d}\rangle \otimes \left(\frac{1}{\sqrt{q^{k-L}}} \sum_{\mathbf{c} \in D_k(\mathbf{d}, \mathbf{s})} |P_{\mathbf{c}}(\mathbf{y})\rangle \right) \right) \\ &= \frac{1}{\sqrt{q^{k-i}}} \sum_{\mathbf{s} \in \mathbb{F}_q^i} \sum_{\mathbf{d} \in \mathbb{F}_q^{L-i}} \sum_{\mathbf{c} \in D_k(\mathbf{d}, \mathbf{s})} a_{\mathbf{s}} |\mathbf{d}, P_{\mathbf{c}}(\mathbf{y})\rangle \\ &= \frac{1}{\sqrt{q^{k-i}}} \sum_{\mathbf{s} \in \mathbb{F}_q^i} \sum_{\mathbf{d} \in \mathbb{F}_q^{L-i}} \sum_{\mathbf{c} \in D_k(\mathbf{d}, \mathbf{s})} a_{\mathbf{s}} |P_{\mathbf{c}}(\mathbf{x}_{\bar{\mathcal{I}}}), P_{\mathbf{c}}(\mathbf{y})\rangle, \end{aligned} \quad (20)$$

where (\mathbf{d}, \mathbf{s}) signifies the horizontal concatenation of \mathbf{d} , and \mathbf{s} , creating one vector of length L . The second step in (20) comes from the definition of $D_k(\mathbf{v} = (v_1, \dots, v_L))$

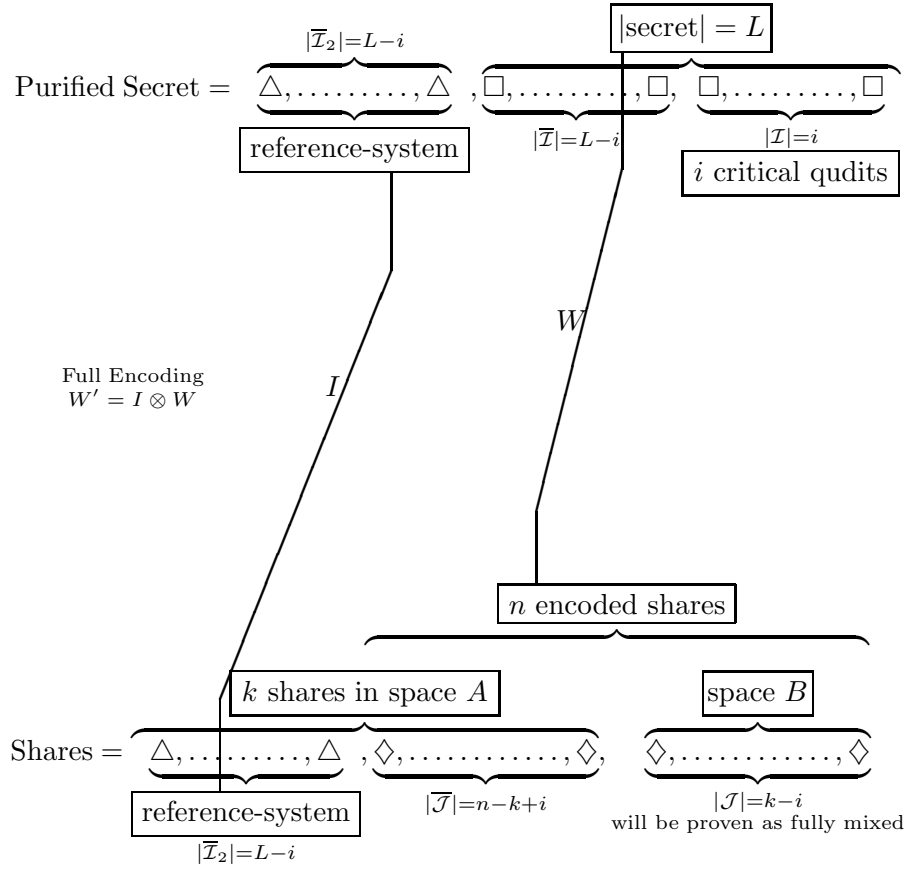


Fig. 1 Strong Security Schematic. L qudits and a reference system of $L-i$ qudits are encoded through W' , to result in n shares and the reference system. Recall that W is the encoding map defined in (2), while I is the identity map. The qudits in space $B = \bigotimes_{j \in \mathcal{J}} \mathcal{H}_j$ are the fully mixed state and have zero information about the i critical qudits of the secret. \triangle represents the reference system qudits, \square represents the secret qudits, and \diamond represents the encoded shares.

as the set of polynomial coefficients such that the evaluation of the polynomial on \mathbf{x} is equal to \mathbf{v} .

We now re-express (20) into the following:

$$\begin{aligned}
 |\psi_{enc}\rangle &= \frac{1}{\sqrt{q^{k-i}}} \sum_{\mathbf{s} \in \mathbb{F}_q^i} \sum_{\mathbf{d} \in \mathbb{F}_q^{L-i}} \sum_{\mathbf{c} \in D_k(\mathbf{d}, \mathbf{s})} a_{\mathbf{s}} |P_{\mathbf{c}}(\mathbf{x}_{\overline{I}}), P_{\mathbf{c}}(\mathbf{y}_{\overline{J}}), P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle \\
 &= \frac{1}{\sqrt{q^{k-i}}} \sum_{\mathbf{g} \in \mathbb{F}_q^L} \sum_{\mathbf{c} \in D_k(\mathbf{g})} a_{\mathbf{g}_I} |P_{\mathbf{c}}(\mathbf{x}_{\overline{I}}), P_{\mathbf{c}}(\mathbf{y}_{\overline{J}}), P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle,
 \end{aligned} \tag{21}$$

where $\mathbf{g} = (\mathbf{d}, \mathbf{s})$, $\mathbf{g}_I = \mathbf{s}$, and $\mathbf{g}_{\overline{I}} = \mathbf{d}$. Note that the number of shares in space A is equal to the length of the vector $(P_{\mathbf{c}}(\mathbf{x}_{\overline{I}}), P_{\mathbf{c}}(\mathbf{y}_{\overline{J}}))$. This length is $|\overline{I}| + |\overline{J}| = (L-i) + (n-k+i)$. Since $n-k = k-L$, the number of shares in space A are

$L - i + k - L + i = k$. Therefore $(P_{\mathbf{c}}(\mathbf{x}_{\mathcal{I}}), P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}}))$ is a vector of k evaluations of the polynomial, specified by \mathbf{c} , on pairwise distinct elements of \mathbf{F}_q . By Lemma 1 this uniquely specifies the polynomial, and therefore \mathbf{c} as well.

We can now calculate the density operator $\rho_{enc} = |\psi_{enc}\rangle\langle\psi_{enc}|$ in (22).

$$\rho_{enc} = \frac{1}{q^{k-i}} \sum_{\mathbf{h}, \mathbf{g} \in \mathbf{F}_q^L} \sum_{\substack{\mathbf{c}_1 \in D_k(\mathbf{g}) \\ \mathbf{c}_2 \in D_k(\mathbf{h})}} a_{\mathbf{g}_I} a_{\mathbf{h}_I}^\dagger |P_{\mathbf{c}_1}(\mathbf{x}_{\mathcal{I}}, \mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}_2}(\mathbf{x}_{\mathcal{I}}, \mathbf{y}_{\mathcal{J}})| \otimes |P_{\mathbf{c}_1}(\mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}_2}(\mathbf{y}_{\mathcal{J}})| \quad (22)$$

The notation $|P_{\mathbf{c}_1}(\mathbf{x}_{\mathcal{I}}, \mathbf{y}_{\mathcal{J}})\rangle$ is written as $|P_{\mathbf{c}_1}(\mathbf{x}_{\mathcal{I}}, \mathbf{y}_{\mathcal{J}})\rangle$ for visibility purposes. Now we perform the partial trace over space A on ρ_{enc} to obtain

$$\begin{aligned} \text{Tr}_A[\rho_{enc}] &= \frac{1}{q^{k-i}} \sum_{\mathbf{h}, \mathbf{g} \in \mathbf{F}_q^L} a_{\mathbf{g}_I} a_{\mathbf{h}_I}^\dagger \sum_{\substack{\mathbf{c}_1 \in D_k(\mathbf{g}) \\ \mathbf{c}_2 \in D_k(\mathbf{h})}} \overbrace{\text{Tr} \left[\frac{|P_{\mathbf{c}_1}(\mathbf{x}_{\mathcal{I}}, \mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}_2}(\mathbf{x}_{\mathcal{I}}, \mathbf{y}_{\mathcal{J}})|}{|P_{\mathbf{c}_1}(\mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}_2}(\mathbf{y}_{\mathcal{J}})|} \right]}^{=\delta_{\mathbf{c}_1, \mathbf{c}_2}} \\ &= \frac{1}{q^{k-i}} \sum_{\mathbf{h}, \mathbf{g} \in \mathbf{F}_q^L} a_{\mathbf{g}_I} a_{\mathbf{h}_I}^\dagger \sum_{\substack{\mathbf{c}_1 \in D_k(\mathbf{g}) \\ \mathbf{c}_2 \in D_k(\mathbf{h})}} \delta_{\mathbf{c}_1, \mathbf{c}_2} |P_{\mathbf{c}_1}(\mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}_2}(\mathbf{y}_{\mathcal{J}})|. \end{aligned} \quad (23)$$

The trace evaluates to the delta function because as noted earlier, the space A contains k evaluations of a polynomial, which, by Lemma 1, specifies \mathbf{c} its coefficients.

Note that for all $\mathbf{g}, \mathbf{h} \in \mathbf{F}_q^L$, the intersection of $D_k(\mathbf{g})$ and $D_k(\mathbf{h})$ is empty if and only if $\mathbf{g} \neq \mathbf{h}$. The traced state (23) is therefore equal to

$$\begin{aligned} \text{Tr}_A[\rho_{enc}] &= \frac{1}{q^{k-i}} \sum_{\mathbf{g} \in \mathbf{F}_q^L} |a_{\mathbf{g}_I}|^2 \sum_{\mathbf{c} \in D_k(\mathbf{g})} |P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})| \\ &= \frac{1}{q^{k-i}} \sum_{\mathbf{s} \in \mathbf{F}_q^i} |a_{\mathbf{s}}|^2 \sum_{\mathbf{d} \in \mathbf{F}_q^{L-i}} \sum_{\mathbf{c} \in D_k(\mathbf{d}, \mathbf{s})} |P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})| \\ &= \frac{1}{q^{k-i}} \sum_{\mathbf{s} \in \mathbf{F}_q^i} |a_{\mathbf{s}}|^2 \sum_{\mathbf{c} \in E_k(\mathbf{s})} |P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})\rangle\langle P_{\mathbf{c}}(\mathbf{y}_{\mathcal{J}})|, \end{aligned} \quad (24)$$

where $E_k(\mathbf{s}) = \{\mathbf{c} \in \mathbf{F}_q^k \mid P_{\mathbf{c}}(\mathbf{x}_{\mathcal{I}}) = \mathbf{s}\}$. By the same argument that equates (8) to (11), (24) is equivalent to

$$\begin{aligned} \text{Tr}_A[\rho_{enc}] &= \frac{1}{q^{k-i}} \sum_{\mathbf{s} \in \mathbf{F}_q^i} |a_{\mathbf{s}}|^2 \sum_{\mathbf{v} \in \mathbf{F}_q^{k-i}} |\mathbf{v}\rangle\langle\mathbf{v}| \\ &= \frac{1}{q^{k-i}} \sum_{\mathbf{v} \in \mathbf{F}_q^{k-i}} |\mathbf{v}\rangle\langle\mathbf{v}|, \end{aligned} \quad (25)$$

which can easily be seen as the fully mixed state in space B . Since this subsystem is the fully mixed state, it must be independent of the secret $|\mathbf{s}_{\mathcal{I}}\rangle$. Thus Condition 2 is satisfied, and our encoder has quantum strong security.

Example 4 We now provide a concrete example of the strong security in a $(k = 3, L = 2, n = 4)$ quantum ramp secret sharing scheme. We retain the notations in this section. Let $q = 7$ be the dimension of each qudit. The public values \mathbf{x} and \mathbf{y} are $\mathbf{x} = (1, 3)$, and $\mathbf{y} = (6, 2, 4, 5)$. Let $\mathcal{I} = \{2\}$, be the index of the qudit of the secret that an unqualified set of participants wants to steal. Let the set of unqualified participants be $\mathcal{J} = \{3, 4\}$. By the strong security condition, the shares 3 and 4 must be unable to produce any information on the second qudit. Let the second qudit be $|s_2 = 5\rangle$. The full secret, including the reference system is therefore

$$|\psi_{\text{pure}}\rangle = \frac{1}{\sqrt{7}}(|0, 0, 5\rangle + |1, 1, 5\rangle + |2, 2, 5\rangle + |3, 3, 5\rangle + |4, 4, 5\rangle + |5, 5, 5\rangle + |6, 6, 5\rangle).$$

By applying the proposed encoding, we arrive at a state which is a superposition of $q^2 = 49$ basis states. We explicitly show 7 basis states out of 49, which come from encoding $|1, 1, 5\rangle$. Recall that the encoder only acts on $L = 2$ qudits, which in this case is the last two qudits $|1, 5\rangle$. We have already shown the encoded state of this is $|\psi_{ex}\rangle$ in (4). Therefore, the encoded state is

$$|1\rangle \otimes |\psi_{ex}\rangle,$$

a superposition of 7 basis states. One can verify that the entire superposition of 49 basis states is

$$\begin{aligned} |\psi_{\text{sec-enc}}\rangle = & \frac{|0\rangle}{7} \otimes (|2, 6, 4, 3\rangle + |3, 5, 0, 4\rangle + |4, 4, 3, 5\rangle + |5, 3, 6, 6\rangle + |6, 2, 2, 0\rangle + |0, 1, 5, 1\rangle + |1, 0, 1, 2\rangle) + \\ & \frac{|1\rangle}{7} \otimes (|\psi_{ex}\rangle) + \\ & \frac{|2\rangle}{7} \otimes (|6, 0, 3, 1\rangle + |0, 6, 6, 2\rangle + |1, 5, 2, 3\rangle + |2, 4, 5, 4\rangle + |3, 3, 1, 5\rangle + |4, 2, 4, 6\rangle + |5, 1, 0, 0\rangle) + \\ & \frac{|3\rangle}{7} \otimes (|1, 4, 6, 0\rangle + |2, 3, 2, 1\rangle + |3, 2, 5, 2\rangle + |4, 1, 1, 3\rangle + |5, 0, 4, 4\rangle + |6, 6, 0, 5\rangle + |0, 5, 3, 6\rangle) + \\ & \frac{|4\rangle}{7} \otimes (|3, 1, 2, 6\rangle + |4, 0, 5, 0\rangle + |5, 6, 1, 1\rangle + |6, 5, 4, 2\rangle + |0, 4, 0, 3\rangle + |1, 3, 3, 4\rangle + |2, 2, 6, 5\rangle) + \\ & \frac{|5\rangle}{7} \otimes (|5, 5, 5, 5\rangle + |6, 4, 1, 6\rangle + |0, 3, 4, 0\rangle + |1, 2, 0, 1\rangle + |2, 1, 3, 2\rangle + |3, 0, 6, 3\rangle + |4, 6, 2, 4\rangle) + \\ & \frac{|6\rangle}{7} \otimes (|0, 2, 1, 4\rangle + |1, 1, 4, 5\rangle + |2, 0, 0, 6\rangle + |3, 6, 3, 0\rangle + |4, 5, 6, 1\rangle + |5, 4, 2, 2\rangle + |6, 3, 5, 3\rangle). \end{aligned}$$

As in Section 6, we now show that the subsystem in space \mathbf{Y} of the shares $|\psi_{\text{sec-enc}}\rangle\langle\psi_{\text{sec-enc}}|$ is the fully mixed state. This is equivalent to showing that the last two qudits are fully mixed. It can be observed that the basis indices of any 3 qudits are unique. For our case, let the first three qudits be traced out. We can verify that the remaining 2 qudits have basis indices filling the entire set $\{(0, 0), (0, 1), \dots, (6, 6)\}$. Thus the qudits in space \mathbf{Y} are fully mixed. In other words, they have no information about the secret $|s_{\mathcal{I}}\rangle$.

7 Conclusion

In this paper, we have shown that Ogawa et al.'s secret sharing scheme does not satisfy the strong security condition for quantum ramp secret sharing. We have provided

a quantum strongly secure ramp secret sharing scheme based on its classical analog. The difference between this encoding and Ogawa et al.'s encoding, is that the secret is encoded into evaluations of polynomials instead of their coefficients. We have provided a decoding method so that, given any k shares, the secret can be reconstructed. Finally we proved that this encoding method is strongly secure by showing that any $k - i$ encoded shares form a fully mixed state. Numerical examples are provided for each proof. The coding efficiency of our encoding is the same as that of the conventional quantum ramp SSs in [10].

Acknowledgements This research was conducted as part of Tokyo Institute of Technology International Research Opportunities Program under Re-Inventing Japan Project funded by Ministry of Education, Culture, Sports, Science and Technology.

This research is partly supported by the National Institute of Information and Communications Technology, Japan, and by the Japan Society for the Promotion of Science Grant Nos. 23246071 and 26289116.

References

1. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.
2. Blakley, G.R., Meadows, C.: Security of ramp schemes. In: *Advances in Cryptology—CRYPTO'84, Lecture Notes in Computer Science*, vol. 196, pp. 242–269. Springer-Verlag (1985). DOI 10.1007/3-540-39568-7_20
3. Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: On the size of shares for secret sharing schemes. *J. Cryptology* **6**(3), 157–167 (1993). DOI 10.1007/BF00198463
4. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. *Phys. Rev. Lett.* **83**(3), 648–651 (1999). DOI 10.1103/PhysRevLett.83.648
5. Gottesman, D.: Theory of quantum secret sharing. *Phys. Rev. A* **61**(4), 042311 (2000). DOI 10.1103/PhysRevA.61.042311
6. Iwamoto, M., Yamamoto, H.: Strongly secure ramp secret sharing schemes for general access structures. *Inform. Process. Lett.* **97**(2), 52–57 (2006). DOI 10.1016/j.ipl.2005.09.012
7. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. *Comm. ACM* **24**(9), 583–584 (1981). DOI 10.1145/358746.358762
8. Nishiara, M., Takizawa, K.: Strongly secure secret sharing scheme with ramp threshold based on Shamir's polynomial interpolation scheme. *Trans. IEICE* **J92-A**(12), 1009–1013 (2009). URL <http://ci.nii.ac.jp/naid/110007483234/en>
9. Ogata, W., Kurosawa, K., Tsujii, S.: Nonperfect secret sharing schemes. In: *Advances in Cryptology – AUSCRYPT '92, Lecture Notes in Computer Science*, vol. 718, pp. 56–66. Springer-Verlag (1993). DOI 10.1007/3-540-57220-1_52
10. Ogawa, T., Sasaki, A., Iwamoto, M., Yamamoto, H.: Quantum secret sharing schemes and reversibility of quantum operations. *Phys. Rev. A* **72**(3), 032318 (2005). DOI 10.1103/PhysRevA.72.032318
11. Shamir, A.: How to share a secret. *Comm. ACM* **22**(11), 612–613 (1979)
12. Smith, A.D.: Quantum secret sharing for general access structures (2000). arXiv:quant-ph/0001087
13. Stinson, D.R.: *Cryptography Theory and Practice*, 3rd edn. Chapman & Hall/CRC (2006)
14. Yamamoto, H.: Secret sharing system using (k, l, n) threshold scheme. *Electronics and Communications in Japan (Part I: Communications)* **69**(9), 46–54 (1986). DOI 10.1002/ecja.4410690906. (the original Japanese version published in 1985)